Listing of Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (currently amended): A method for performing a cryptographic operation in a device under [[the]] control of a security application , in which a cryptographic value (y) is produced in the device, by a calculation utilizing a processor comprising at least one multiplication operation between a first (f_1) and a second (f_2) factor ~~two factors~~ including a part at least of a secret key (s) associated with the device, the method comprising:

selecting and memorizing the first factor as ~~wherein the first of the two factors of the multiplication has~~ a determined number of bits L in binary representation; [[,]]

selecting and memorizing the second factor so as to comprise a ~~the second of the two factors of the multiplication is constrained so that it comprises, in~~ binary representation having [[,]] several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L – 1 bits set to 0; [[,]]

carrying out the multiplication operation by assembling successive shifted versions of the selected and memorized shifted binary versions of the first factor, thereby allowing said cryptographic operation to be conducted in the absence of any completed effective multiplication operation due to said shifting and assembling. ~~and the multiplication is achieved by assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor~~.

Claim 2 (previously presented): The method as claimed in claim 1, in which the secret key (s) forms part of an asymmetric cryptographic key pair associated with the device .

Claim 3 (previously presented): The method as claimed in claim 1 , in which the device comprises a chip including hard-wired logic for producing the cryptographic value.

Claim 4 (previously presented): The method as claimed in claim 1, in which the calculation of the cryptographic value furthermore comprises an addition or a subtraction between a pseudo-random number (r) and the result of the multiplication.

Claim 5 (currently amended): The method as claimed in claim 4, in which the first and second factors (f_1, f_2 [[s, c]]) and the pseudo-random number (r) are dimensioned so that the pseudo-random number is greater than the result of the multiplication.

Claim 6 (original): The method as claimed in claim 5, in which the number of bits set to 1 of the second factor is chosen at most equal to the largest integer less than or equal to s_1/L, where s_1 is a predefined threshold less than the number of bits of the pseudo-random number (r) in binary representation.

Claim 7 (previously presented): The method as claimed in claim 1, in which the two factors of the multiplication include, as well as said part of the secret key (s), a number (c) provided to the device by the security application executed outside the device.

Claim 8 (previously presented): The method as claimed in claim 1, in which the two factors of the multiplication include, as well as said secret key (s), a number (c) provided by the device.

Claim 9 (currently amended): The method as claimed in claim 1, in which said part of the secret key (s) is said first factor (f_1) of the multiplication.

Claim 10 (currently amended): The method as claimed in claim 1 [[9]], the method further comprising:

calculating ~~in which said binary versions are disposed in respective~~ intervals of like size in bits, said size corresponding to the total size of a usable space [[,]] divided by the number of bits set to 1 of the second factor of the multiplication operation; [[,]]

placing each shifted binary version ~~being placed~~ in its respective interval as a function of a shift in accordance with the positions of the bits set to 1 of the second factor.

Claim 11 (currently amended): The method as claimed in claim 1, in which said part of the secret key (s) is the second factor (f_2) of the multiplication.

Claim 12 (original): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding the positions of its bits set to 1.

Claim 13 (currently amended): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding numbers of bits separating respectively lower bounds of intervals of (S-1)/(n-1) bits and lower bounds of blocks of bits allotted to the first factor (f_1 [[c]]) of the multiplication and each disposed in the associated intervals, S being the number of bits of the secret key (s) and n the number of bits set to 1 of the secret key (s).

Claim 14 (currently amended): The method as claimed in claim 11, in which the secret key (s) is stored in a memory support of the device by coding numbers of bits, each representative of the number of bits separating two blocks of successive bits allotted to the first factor (f_1 [[c]]) of the multiplication.

Claim 15 (previously presented): The method as claimed in claim 1, in which the cryptographic value (y) is produced so as to authenticate the device in a transaction with the security application executed outside the device.

Claim 16 (previously presented): The method as claimed in claim 1, in which the cryptographic value (y) is produced in the guise of electronic signature.

Claim 17 (currently amended): A device with cryptographic function, comprising:

means of interfacing with a security application; and

means of calculation for producing a cryptographic value (y), the means of calculation comprising means of multiplication between a first (f_1) and second (f_2) [[two]] factors including a part at least of a secret key (s) associated with the device, wherein, a first factor (f_1) has ~~of the two factors of the multiplication having~~ a determined number of bits L in binary representation, and the second factor

(f_2) ~~of the two factors of the multiplication~~ being constrained so that it comprises, in binary representation, several bits set to 1 with, between each pair of consecutive bits set to 1, a sequence of at least L – 1 bits set to 0; [[,]]

means for selecting and memorizing successive binary versions of the first factor by shifting said first factor in accordance with the positions of the bits set to 1 of the second factor; and

means for assembling the successive shifted versions of the selected and memorized shifted binary versions of the first factor, said means for assembling allowing said cryptographic operation to be conducted in an absence of any completed effective multiplication operation.

~~the multiplication means comprise means for assembling binary versions of the first factor, respectively shifted in accordance with the positions of the bits set to 1 of the second factor.~~

Claim 18 (previously presented): The device as claimed in claim 17, furthermore comprising means of generating a pseudo-random number (r), the means of calculation comprising means for adding the result of the multiplication to or subtracting it from said pseudo-random number.

Claim 19 (currently amended): The device as claimed in claim 18, in which the first and second factors (f_1, f_2 [[s, c]]) and the pseudo-random number (r) are dimensioned so that the pseudo-random number is greater than the result of the multiplication.

Claim 20 (previously presented): The device as claimed in claim 17, in which the means of calculation are embodied as hard-wired logic.

Claim 21 (currently amended): The device as claimed in claim 17, in which said part of the secret key (s) is the first factor (f_1) of the multiplication.

Claim 22 (currently amended): The device as claimed in claim 17, in which said part of the secret key (s) is the second factor (f_2) of the multiplication.

Claim 23 (previously presented): The device as claimed in claim 22, furthermore comprising a memory adapted for storing data for coding the positions of the bits set to 1 of the secret key (s).